

JP10260939

Publication Title:

**CLIENT MACHINE AUTHENTICATION METHOD OF COMPUTER NETWORK,
CLIENT MACHINE, HOST MACHINE AND COMPUTER SYSTEM**

Abstract:

Abstract of JP10260939

PROBLEM TO BE SOLVED: To prevent an invalid user from invading to a network by a host machine deciding whether machine inherent information that is sent from a client machine that makes an access request coincides with machine inherent information that is registered in accordance with a user's ID which is simultaneously sent or not. **SOLUTION:** A client machine CM sends a user's ID and a password, and a host machine HM collates whether the sent user's ID is registered in a user's database 10 or not and identify the user to a communication of the machine CM side. When a user's ID is unmatching, the machine HM requests the machine CM to resend this user's ID, and if it is unmatching again, the machine HM disconnects the line. In the case of matching, after that, the access of the machine CM to the machine HM is allowed. However, if it is unmatching, a regular access is not allowed, and, for instance, a temporary access is allowed.

Data supplied from the esp@cenet database - Worldwide

Courtesy of <http://v3.espacenet.com>

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-260939

(43)公開日 平成10年(1998) 9月29日

(51)Int.Cl. ⁶	識別記号	F I	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C
			3 3 0 B
13/00	3 5 7	13/00	3 5 7 Z

審査請求 未請求 請求項の数17 O L (全 18 頁)

(21)出願番号 特願平9-67008

(22)出願日 平成9年(1997) 3月19日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 河合 淳

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 矢崎 孝一

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 弁理士 河野 登夫

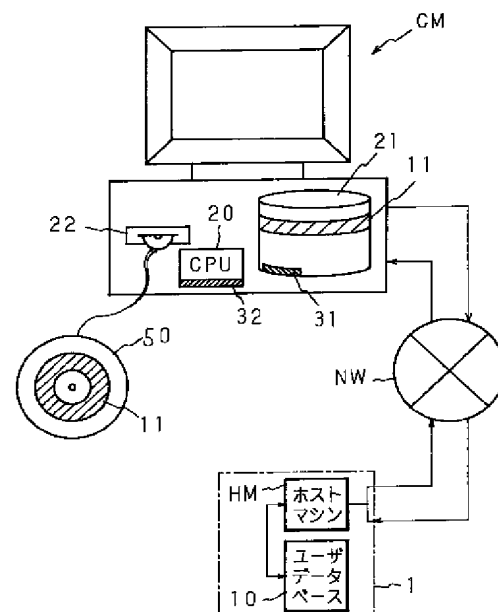
(54)【発明の名称】 コンピュータネットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン
及びコンピュータシステム

(57)【要約】

【課題】 パソコン通信においては、セキュリティ確保のために認証方法が採用されている。しかし、ユーザIDとパスワードのみによる従来の認証方法では、パスワードにユーザ自身の誕生日等のような判明し易い数字が使用されたり、あるいはパスワードをユーザがメモ書きしてモニタに貼ってあったり等、ユーザによるパスワード管理に問題が多いため、十分な認証機能を果たせてはいないという課題があった。

【解決手段】 ホストマシンHMでユーザデータベース10を参照することにより、マシン固有情報(たとえばHDD-ID31、CPU-ID32等)を使用してユーザID及びそのユーザが使用するクライアントマシンCMを特定する。

本発明のコンピュータネットワークのクライアントマシン認証方法の実施に使用されるユーザ側のクライアントマシンの構成及びそのネットワーク接続の状態を示す模式図



【特許請求の範囲】

【請求項1】 コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法において、
個々のクライアントマシンに固有のマシン固有情報を、
個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、
個々のクライアントマシンは、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、自身のマシン固有情報を前記ホストマシンへ送信し、
前記ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたマシン固有情報が同時に送信されてきたユーザIDに対応して登録されているマシン固有情報と一致するか否かを判定することを特徴とするコンピュータネットワークのクライアントマシン認証方法。

【請求項2】 コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法において、
個々のクライアントマシンに固有のマシン固有情報を、
個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、
前記ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておき、
個々のクライアントマシンは、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、前記ホストマシンから予め送付されているアクセスコードファイルを前記ホストマシンへ送信し、
前記ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを前記秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とするコンピュータネットワークのクライアントマシン認証方法。

【請求項3】 コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法において、
個々のクライアントマシンに固有のマシン固有情報を、
個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、
前記ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておき、

前記クライアントマシンは、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、前記ホストマシンから予め送付されているアクセスコードファイル及びマシン固有情報を前記ホストマシンへ送信し、
前記ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを前記秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とするコンピュータネットワークのクライアントマシン認証方法。

【請求項4】 コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法において、
個々のクライアントマシンに固有のマシン固有情報を、
個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、
前記ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておき、個々のクライアントマシンからのアクセス要求時に、アクセス要求しているクライアントマシンのマシン固有情報を含む公開鍵を生成し、生成した公開鍵のマシン固有情報以外の部分をクライアントマシンへ送信し、
アクセス要求しているクライアントマシンは、入力されたユーザIDを前記ホストマシンへ送信すると共に、前記ホストマシンから受信した公開鍵の一部と自身のマシン固有情報とから前記公開鍵を復元し、前記ホストマシンから予め送付されているアクセスコードファイル及び／又は自身のマシン固有情報を復元した公開鍵で暗号化して前記ホストマシンへ送信し、
前記ホストマシンは、アクセス要求しているクライアントマシンから送信されてきた公開鍵暗号の秘密鍵で暗号化されたアクセスコードファイル及び／又はマシン固有情報を前記秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とするコンピュータネットワークのクライアントマシン認証方法。

【請求項5】 前記アクセスコードファイルは、前記クライアントマシンからのアクセス要求に対して前記ホストマシンがアクセスを許可する都度、前記ホストマシンにより変更されることを特徴とする請求項2乃至4のいずれかに記載のコンピュータネットワークのクライアン

トマシン認証方法。

【請求項6】 前記クライアントマシンは、ハードウェア階層に保持されている前記マシン固有情報を読み出すマシン固有情報の第1の読み出し手段をオペレーティングシステム階層に、前記ホストマシンへ前記マシン固有情報を送信すべく、前記第1の読み出し手段から読み出す第2の読み出し手段をアプリケーション階層にそれぞれ備え、更に、前記第1の読み出し手段及び前記第2の読み出し手段相互間での通信を相互に認証するための認証手段を前記オペレーティングシステム階層及びアプリケーション階層にそれぞれ備えたことを特徴とする請求項1乃至4のいずれかに記載のコンピュータネットワークのクライアントマシン認証方法。

【請求項7】 個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、自身のマシン固有情報を前記ホストマシンへ送信すべくしてあることを特徴とするクライアントマシン。

【請求項8】 個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、前記ホストマシンから予め送付されているアクセスコードファイルを前記ホストマシンへ送信すべくしてあることを特徴とするクライアントマシン。

【請求項9】 個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、前記ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、前記ホストマシンから予め送付されているアクセスコードファイル及びマシン固有情報を前記ホストマシンへ送信すべくしてあることを特徴とするクライアントマシン。

【請求項10】 個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであっ

て、

アクセス要求時に、入力されたユーザIDを前記ホストマシンへ送信すると共に、前記ホストマシンから受信した公開鍵の一部と自身のマシン固有情報とから前記公開鍵を復元し、前記ホストマシンから予め送付されているアクセスコードファイル及び／又は自身のマシン固有情報を復元した公開鍵で暗号化して前記ホストマシンへ送信すべくしてあることを特徴とするクライアントマシン。

【請求項11】 ハードウェア階層に保持されている前記マシン固有情報を読み出すマシン固有情報の第1の読み出し手段をオペレーティングシステム階層に、前記ホストマシンへ前記マシン固有情報を送信すべく、前記第1の読み出し手段から読み出す第2の読み出し手段をアプリケーション階層にそれぞれ備え、更に、前記第1の読み出し手段及び前記第2の読み出し手段相互間での通信を相互に認証するための認証手段を前記オペレーティングシステム階層及びアプリケーション階層にそれぞれ備えたことを特徴とする請求項7乃至10のいずれかに記載のクライアントマシン。

【請求項12】 コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、前記データベースの登録内容を参照して、アクセス要求しているクライアントマシンから送信されてきたマシン固有情報が同時に送信されてきたユーザIDに対応して登録されているマシン固有情報と一致するか否かを判定する手段とを備えたことを特徴とするホストマシン。

【請求項13】 コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、

少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを前記秘密鍵で復号する手段と、

復号されたアクセス許可情報の真偽を判定する手段と、前記データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とするホストマシン。

【請求項14】 コンピュータネットワークを介してク

クライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを前記秘密鍵で復号する手段と、復号されたアクセス許可情報の真偽を判定する手段と、前記データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とするホストマシン。

【請求項15】 コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、個々のクライアントマシンからのアクセス要求時に、アクセス要求しているクライアントマシンのマシン固有情報を含む公開鍵を生成し、生成した公開鍵のマシン固有情報以外の部分をクライアントマシンへ送信する手段と、アクセス要求しているクライアントマシンから送信されてきた公開鍵暗号の秘密鍵で暗号化されたアクセスコードファイル及び／又はマシン固有情報を前記秘密鍵で復号する手段と、復号されたアクセス許可情報の真偽を判定する手段と、前記データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とするホストマシン。

【請求項16】 前記アクセスコードファイルを、前記クライアントマシンからのアクセス要求に対して前記ホストマシンがアクセスを許可する都度、変更することを特徴とする請求項13乃至15のいずれかに記載のホストマシン。

【請求項17】 ハードウェア階層に固有のマシン固有情報を保持し、オペレーティングシステム階層に備えられた第1の読み出し手段により前記ハードウェア階層に保持されている前記マシン固有情報を読み出し、アプリケーション階層に備えられた第2の読み出し手段により前記第1の読み出し手段が読み出したマシン固有情報を読み出して外部へ出力するコンピュータシステムにおいて、前記オペレーティングシステム階層に第1認証手段を、前記アプリケーション階層に第2の認証手段を備え、前記第1の認証手段は、前記第2の認証手段からの認証要求に応じて第1の乱数を発生して前記第2の認証手段へ送信し、前記第2の認証手段は、受信した第1の乱数と自身で発生した第2の乱数との間で所定の演算を行なってその演算結果及び前記第2の乱数を前記第1の認証手段へ送信し、前記第1の認証手段は、受信した演算結果に前記所定の演算の逆演算を行なってその結果と受信した前記第2の乱数とを比較し、一致した場合に前記第1の乱数と前記第2の乱数との間で前記所定の演算を行なってその演算結果及び前記第1の乱数を前記第2の認証手段へ送信し、前記第2の認証手段は、受信した演算結果に前記所定の演算の逆演算を行なってその結果と受信した前記第1の乱数とを比較し、一致した場合に相互認証が完了したと判断して前記第1の読み出し手段から前記第2の読み出し手段へのマシン固有情報の送信を行なうべくしてあることを特徴とするコンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータシステム、特にパーソナルコンピュータシステムを使用した通信、例えばパソコン通信等のコンピュータネットワーク通信におけるクライアントマシンの認証方法に関し、更にそのような認証方法を実施するためのクライアントマシン、ホストマシン及びコンピュータシステムに関する。

【0002】

【従来の技術】近年のコンピュータ技術の発展に伴って、特に大容量高速通信技術及び操作が容易な種々の通信ソフトウェアの開発に伴って、多くの人々がインターネット等のパソコン通信を日常的に利用するようになっている。

【0003】

【発明が解決しようとする課題】ところで、上述のようなパソコン通信においては、セキュリティ確保のために認証方法が採用されている。しかし、ユーザIDとパスワードのみによる従来の認証方法では、パスワードにユーザ自身の誕生日等のような判明し易い数字が使用され

たり、あるいはパスワードをユーザがメモ書きしてモニタに貼ってあったり等、ユーザによるパスワード管理に問題が多いため、十分な認証機能を果たせてはいないというのが実情である。

【0004】また、発信元の電話番号をチェックして正規のユーザであるかを調べる方法もあるが、この方法では携帯型のパーソナルコンピュータを所持するユーザが移動中に公衆回線を利用する場合等のようないわゆるモバイル環境下においては利用出来ない。またこの手法では、不正アクセス確認のために前回のアクセス時の電話番号を表示するため、逆に不正使用者に正規ユーザの電話番号を知らせることになるという問題もあった。

【0005】本発明は上述のような事情に鑑みてなされたものであり、今後益々増加すると考えられるモバイル環境にも対応可能な認証方法の強化と、マシン固有の情報を利用して正規ユーザが使用するマシンを特定することにより、正規ユーザのプライバシーの保護、不正使用常習者のネットワークへの侵入防止を可能とするコンピュータネットワークのクライアントマシン認証方法の提供を目的とする。

【0006】

【課題を解決するための手段】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第1の発明は、コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法であって、個々のクライアントマシンに固有のマシン固有情報を、個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、個々のクライアントマシンは、ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、自身のマシン固有情報をホストマシンへ送信し、ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたマシン固有情報が同時に送信されてきたユーザIDに対応して登録されているマシン固有情報と一致するか否かを判定することを特徴とする。

【0007】本発明に係るクライアントマシンの第1の発明は、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、自身のマシン固有情報をホストマシンへ送信すべくしてあることを特徴とする。

【0008】本発明に係るホストマシンの第1の発明は、コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを

対応付けて予め登録したデータベースと、データベースの登録内容を参照して、アクセス要求しているクライアントマシンから送信されてきたマシン固有情報が同時に送信されてきたユーザIDに対応して登録されているマシン固有情報と一致するか否かを判定する手段とを備えたことを特徴とする。

【0009】このような本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン及びホストマシンの第1の発明では、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報がホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定する。

【0010】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第2の発明は、コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法であって、個々のクライアントマシンに固有のマシン固有情報を、個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておき、ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておき、個々のクライアントマシンは、ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、ホストマシンから予め送付されているアクセスコードファイルをホストマシンへ送信し、ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とする。

【0011】本発明に係るクライアントマシンの第2の発明は、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、ホストマシンから予め送付されているアクセスコードファイルをホストマシンへ送信すべくしてあることを特徴とする。

【0012】本発明に係るホストマシンの第2の発明は、コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、少なくとも個

々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを秘密鍵で復号する手段と、復号されたアクセス許可情報の真偽を判定する手段と、データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とする。

【0013】このような本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン及びホストマシンの第2の発明では、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、予めホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとがホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定する。

【0014】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第3の発明は、コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法であって、個々のクライアントマシンに固有のマシン固有情報を、個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておく、ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておく、クライアントマシンは、ホストマシンへのアクセス要求時に、入力されたユーザIDと共に、ホストマシンから予め送付されているアクセスコードファイル及びマシン固有情報をホストマシンへ送信し、ホストマシンは、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とする。

【0015】本発明に係るクライアントマシンの第3の発明は、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、ホストマシンへのアクセス要求時に、入力されたユーザIDと

共に、ホストマシンから予め送付されているアクセスコードファイル及びマシン固有情報をホストマシンへ送信すべくしてあることを特徴とする。

【0016】本発明に係るホストマシンの第3の発明は、コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、アクセス要求しているクライアントマシンから送信されてきたアクセスコードファイルを秘密鍵で復号する手段と、復号されたアクセス許可情報の真偽を判定する手段と、データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とする。

【0017】このような本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン及びホストマシンの第3の発明では、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報と予めホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとがホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定する。

【0018】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第4の発明は、コンピュータネットワークを介してクライアントマシンとホストマシンとが通信する際のクライアントマシン認証方法であって、個々のクライアントマシンに固有のマシン固有情報を、個々のクライアントマシンを使用するユーザのユーザIDと対応付けて予めホストマシン側に登録しておく、ホストマシンは、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付しておく、個々のクライアントマシンからのアクセス要求時に、アクセス要求しているクライアントマシンのマシン固有情報を含む公開鍵を生成し、生成した公開鍵のマシン固有情報以外の部分をクライアントマシンへ送信し、アクセス要求しているクライアントマシンは、入力されたユーザIDをホストマシンへ送信すると共に、ホストマシンから受信した公開鍵の一部と自身のマシン固有情報とから公開鍵を復元し、ホストマシンから予め送付されているアクセスコードファイル及び／又は

自身のマシン固有情報を復元した公開鍵で暗号化してホストマシンへ送信し、ホストマシンは、アクセス要求しているクライアントマシンから送信されてきた公開鍵暗号の秘密鍵で暗号化されたアクセスコードファイル及び／又はマシン固有情報を秘密鍵で復号し、復号されたアクセス許可情報の真偽を判定すると共に、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定することを特徴とする。

【0019】本発明に係るクライアントマシンの第4の発明は、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースを備えたホストマシンとコンピュータネットワークを介して通信するクライアントマシンであって、アクセス要求時に、入力されたユーザIDをホストマシンへ送信すると共に、ホストマシンから受信した公開鍵の一部と自身のマシン固有情報とから公開鍵を復元し、ホストマシンから予め送付されているアクセスコードファイル及び／又は自身のマシン固有情報を復元した公開鍵で暗号化してホストマシンへ送信すべくしてあることを特徴とする。

【0020】本発明に係るホストマシンの第4の発明は、コンピュータネットワークを介してクライアントマシンと通信するホストマシンであって、個々のクライアントマシンに付与された固有のマシン固有情報と、個々のクライアントマシンを使用するユーザのユーザIDとを対応付けて予め登録したデータベースと、少なくとも個々のクライアントマシンのマシン固有情報と個々のクライアントマシンに対するアクセス許可情報とを秘密鍵で暗号化したアクセスコードファイルを作成して個々のクライアントマシンへ予め送付する手段と、個々のクライアントマシンからのアクセス要求時に、アクセス要求しているクライアントマシンのマシン固有情報を含む公開鍵を生成し、生成した公開鍵のマシン固有情報以外の部分をクライアントマシンへ送信する手段と、アクセス要求しているクライアントマシンから送信されてきた公開鍵暗号の秘密鍵で暗号化されたアクセスコードファイル及び／又はマシン固有情報を秘密鍵で復号する手段と、復号されたアクセス許可情報の真偽を判定する手段と、データベースの登録内容を参照して、復号されたマシン固有情報と送信されてきたマシン固有情報とが一致するか否か、復号されたマシン固有情報と送信されてきたユーザIDに対応して登録されているマシン固有情報とが一致するか否かを判定する手段とを備えたことを特徴とする。

【0021】このような本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン及びホストマシンの第4の発明では、クライアントマ

シンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報と予めホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとが公開鍵で暗号化されてホストマシンへ送信され、ホストマシンでは秘密鍵で復号してデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定する。

【0022】また、上述の各発明において、アクセスコードファイルは、クライアントマシンからのアクセス要求に対してホストマシンがアクセスを許可する都度、ホストマシンにより変更されることを特徴とする。

【0023】従って、上述の各発明ではクライアントマシンからホストマシンへのアクセスが許可される都度、アクセスコードファイルが変更されるため、よりセキュリティが高くなる。

【0024】更に上述の各発明において、クライアントマシンは、ハードウェア階層に保持されているマシン固有情報を読み出すマシン固有情報の第1の読み出し手段をオペレーティングシステム階層に、ホストマシンへマシン固有情報を送信すべく、第1の読み出し手段から読み出す第2の読み出し手段をアプリケーション階層にそれぞれ備え、更に、第1の読み出し手段及び第2の読み出し手段相互間での通信を相互に認証するための認証手段をオペレーティングシステム階層及びアプリケーション階層にそれぞれ備えたことを特徴とする。

【0025】従って、上述の各発明では、クライアントマシンのマシン固有情報自体を改竄することが防止される。

【0026】更に、本発明に係るコンピュータシステムは、ハードウェア階層に固有のマシン固有情報を保持し、オペレーティングシステム階層に備えられた第1の読み出し手段によりハードウェア階層に保持されているマシン固有情報を読み出し、アプリケーション階層に備えられた第2の読み出し手段により第1の読み出し手段が読み出したマシン固有情報を読み出して外部へ出力するコンピュータシステムであって、オペレーティングシステム階層に第1認証手段を、アプリケーション階層に第2の認証手段を備え、第1の認証手段は、第2の認証手段からの認証要求に応じて第1の乱数を発生して第2の認証手段へ送信し、第2の認証手段は、受信した第1の乱数と自身で発生した第2の乱数との間で所定の演算を行なってその演算結果及び第2の乱数を第1の認証手段へ送信し、第1の認証手段は、受信した演算結果に所定の演算の逆演算を行なってその結果と受信した第2の乱数とを比較し、一致した場合に第1の乱数と第2の乱数との間で所定の演算を行なってその演算結果及び第1の乱数を第2の認証手段へ送信し、第2の認証手段は、受信した演算結果に所定の演算の逆演算を行なってその結果と受信した第1の乱数とを比較し、一致した場合に相互認証が完了したと判断して第1の読み出し手段から

第2の読み出し手段へのマシン固有情報の送信を行なうべくしてあることを特徴とする。

【0027】このような本発明のコンピュータシステムでは、ハードウェア階層に保持されているハードディスク、CPU等のIDであるマシン固有情報を外部へ出力する際の改竄が防止される。

【0028】

【発明の実施の形態】以下、本発明をその実施の形態を示す図面に基づいて詳述する。まず最初に、本発明のコンピュータネットワークのクライアントマシン認証方法の実施に使用されるユーザ側のクライアントマシンの構成及びそのネットワーク接続の状態を図1の模式図を参照して説明する。

【0029】図1において、参照符号CMはユーザが使用するクライアントマシンを示しており、基本的には一般的なパーソナルコンピュータである。このクライアントマシンCMはネットワークNWを介して通信センタ1と接続している。なお、図1には示されていないが、通信センタ1にはホストマシンHMが設置されている他、各ユーザのユーザID、マシンの固有情報(HDD-ID、CPU-ID等)が登録されたユーザデータベース10が設置されている。

【0030】クライアントマシンCMには、一般的なコンピュータシステム同様に、CPU20、ハードディスク21、CD-ROMドライブ22等が備えられている。ハードディスク21には固有のID(以下、HDD-IDと言う)31が付与されており、またCPU20にも固有のID(以下、CPU-IDと言う)32が付与されている。なお、このクライアントマシンCMによる通信センタ1との通信は、たとえばCD-ROM50に記録されている通信ソフトウェア11がCD-ROMドライブ22により読み取られてハードディスク21に書き込まれ、それに従ってCPU20が動作することにより実現される。

【0031】図2は本発明に係るコンピュータネットワークのクライアントマシン認証方法の第1の発明の手順を示すフローチャートである。なお、二重ボックスはクライアントマシンCM側でのユーザによる操作及びクライアントマシンCMによる処理を、太線のボックスは通信センタ1に設置されているホストマシンHM側での操作・処理をそれぞれ示している。

【0032】まず、ユーザは自身のクライアントマシンCMからホストマシンHMに回線を接続してアクセスを要求し(ステップS11)、続いてユーザID及びパスワードを送信してユーザ特定シーケンスに入る(ステップS12)。以上のクライアントマシンCM側の通信に対して、ホストマシンHMではまず送信されてきたユーザIDがユーザデータベース10に登録されているか否かを照合し、ユーザを特定する(ステップS1)。但し、一致するユーザIDが見つからない場合には、ホストマシンHMはユーザIDの再送信をクライアントマシンCMに要求し、再度不一致であれば回線を切断する(ステップS2)。

【0033】このようにしてユーザ特定シーケンスにパ

スしたユーザはマシン特定認証シーケンスに入る。まず、ホストマシンHMからクライアントマシンCMに対してマシン固有情報を要求する(ステップS13)。これに対してクライアントマシンCMではマシン固有情報、たとえばHDD-ID31、CPU-ID32のいずれかまたは双方を送信する(ステップS14)。

【0034】以上のようにしてクライアントマシンCMからマシン固有情報がホストマシンHMへ送信されると、ホストマシンHMでは予め個々のユーザが使用するマシン固有情報がユーザデータベース10に登録されているので、先に特定されているユーザIDとマシン固有情報とを照合する。この結果、一致すれば、以降のクライアントマシンCMからホストマシンHMへのアクセスが許可される(ステップS16)。しかし、不一致であれば(ステップS17)、正式のアクセスは許可されず(ステップS18)、たとえば仮アクセスが許可される。

【0035】但し、上述のような本発明のコンピュータネットワークのクライアントマシン認証方法の第1の発明では、クライアントマシンCMとホストマシンHMとの間の通信路の安全性が十分でない場合、またはクライアントマシンCMのマシン固有情報を第三者が入手し易い場合で且つ不正使用者がプログラマレベルであってソフトウェアに精通しているような場合には効果が低い可能性がある。

【0036】図3は本発明に係るコンピュータネットワークのクライアントマシン認証方法の第2の発明の手順を示すフローチャートである。なお、二重ボックスはクライアントマシンCM側でのユーザによる操作・処理を、太線のボックスは通信センタ1に設置されているホストマシンHM側での操作・処理をそれぞれ示している。

【0037】まず、ユーザは自身のクライアントマシンCMからホストマシンHMに回線を接続してアクセスを要求し(ステップS31)、続いてユーザID及びパスワードを送信してユーザ特定シーケンスに入る(ステップS22)。以上のクライアントマシンCM側の通信に対して、ホストマシンHMではまず送信されてきたユーザIDがユーザデータベース10に登録されているか否かを照合し、ユーザを特定する(ステップS1)。但し、一致するユーザIDが見つからない場合には、ホストマシンHMはユーザIDの再送信をクライアントマシンCMに要求し、再度不一致であれば回線を切断する(ステップS2)。

【0038】このようにしてユーザ特定シーケンスにパスしたユーザはマシン特定認証シーケンスに入る。まず、ホストマシンHMからクライアントマシンCMに対してアクセスコードファイルを要求する(ステップS23)。これに対してクライアントマシンCMではアクセスコードファイルを既に所有している場合には送信する(ステップS24)。但し、クライアントマシンCMでアクセスコードファイルを未だ所有していない場合にはその旨を通知する(ステップS25)。この場合には正式のアクセスは許可さ

れないが、仮のアクセスは許可される。この際の処理手順は後述する。

【0039】以上のようにしてクライアントマシンCMからアクセスコードファイルがホストマシンHMへ送信されると、ホストマシンHMでは送られてきたアクセスコードファイルを秘密鍵で復号し（ステップS26）、まず正規のアクセスコードであることを照合する（ステップS27）。この際、アクセスコードが不正であった場合には（ステップS30）、正式のアクセスは許可されない（ステップS32）。

【0040】次にホストマシンHMは復号したアクセスコードに含まれるマシン固有情報を、ユーザデータベース10から先に特定されているユーザIDとマシン固有情報とを照合する（ステップS28）。この結果、一致すれば、以降のクライアントマシンCMからホストマシンHMへのアクセスが許可される（ステップS29）。しかし、不一致であれば（ステップS31）、正式のアクセスは許可されず（ステップS32）、たとえば仮アクセスが許可される。

【0041】次に、クライアントマシンCMからアクセスコードファイルを未だ所有していない旨がホストマシンHMへ通知された場合（ステップS25）、またはアクセスコードが不正であった場合（ステップS32）の後の処理手順について、図4のフローチャートを参照して説明する。

【0042】まずこの場合、アクセスコードファイルを有していないマシン（クライアントマシンCM）に対しては仮登録が、アクセスコードが不正であったマシン（クライアントマシンCM）に対してはアクセスの終了が選択される（ステップS40, S41, S42）。

【0043】仮登録は以下の手順で行なわれる。まず、ホストマシンHMからクライアントマシンCMに対してマシン固有情報が要求されると共にホスト公開鍵が送信される（ステップS42）。これに応じてクライアントマシンCMでは自身のマシン固有情報をホストマシンHMから送られてきたホスト公開鍵で暗号化し（ステップS43）、暗号化した後のマシン固有情報をホストマシンHMへ送信する（ステップS44）。

【0044】ホストマシンHMではクライアントマシンCMから送られてきた暗号化後のマシン固有情報を秘密鍵で復号してそのクライアントマシンCMの固有情報を入手する（ステップS45）。更にホストマシンHMは第2の秘密鍵でアクセス許可情報またはマシン固有情報を暗号化してアクセスコードファイルを作成する（ステップS46）。このアクセスコードファイルはホストマシンHMからクライアントマシンCMへ送信されると共に、ホストマシンHMではユーザデータベース10の対応するユーザIDにリンクさせて仮登録する（ステップS47）。

【0045】但し、上述のような本発明のコンピュータネットワークのクライアントマシン認証方法の第2の発明では、通信路の安全性が十分でない場合、またはクライアントマシンCMのアクセスコードファイルを第三者が

入手し易い場合には効果が低い可能性がある。

【0046】図5、図6及び図7は本発明に係るコンピュータネットワークのクライアントマシン認証方法の第3の発明及び第4の発明の手順を示すフローチャートである。なお、二重ボックスはクライアントマシンCM側でのユーザによる操作・処理を、太線のボックスは通信センタ1に設置されているホストマシンHM側での操作・処理をそれぞれ示している。

【0047】まず、ユーザは自身のクライアントマシンCMからホストマシンHMに回線を接続してアクセスを要求し（ステップS51）、続いてユーザID及びパスワードを送信してユーザ特定シーケンスに入る（ステップS52）。以上のクライアントマシンCM側の通信に対して、ホストマシンHMではまず送信されてきたユーザIDがユーザデータベース10に登録されているか否かを照合し、ユーザを特定する（ステップS1）。但し、一致するユーザIDが見つからない場合には、ホストマシンHMはユーザIDの再送信をクライアントマシンCMに要求し、再度不一致であれば回線を切断する（ステップS2）。

【0048】このようにしてユーザ特定シーケンスにパスしたユーザはマシン特定認証シーケンスに入る。まず、ホストマシンHMからのクライアントマシンに対してマシン固有情報及びアクセスコードファイルを要求すると共に公開鍵を送信する（ステップS53）。これに対してクライアントマシンCMではマシン固有情報（マシン名、CPU-ID、HDD-ID、OS-ID等）を公開鍵暗号化して送信する（ステップS54）と共に、アクセスコードファイルを送信する（ステップS56）。但し、クライアントマシンCMでアクセスコードファイルを未だ所有していない場合にはその旨を通知する（ステップS55）。この場合には正式のアクセスは許可されないが、仮のアクセスは許可される。この際の処理手順は後述する。

【0049】ホストマシンHMでは公開鍵暗号の秘密鍵でマシン固有情報を復号し（ステップS80）、マシン固有情報を不正使用者マシンデータベースで検索し（ステップS81）、不正使用者のマシンであるか否かをチェックし、不正使用者のマシンである場合には不正使用者対応処理に移る（ステップS83）。具体的には、アクセスの拒否、不正ユーザの電話番号登録、不正ユーザの所在の逆探知等の措置を採り得る。一方、不正使用者マシンに該当しない場合には、ホストマシンHMは復号したマシン固有情報をユーザデータベース10に登録されているマシンリストと照合し（ステップS82）、次の処理に移る。

【0050】クライアントマシンCMがアクセスコードファイルを送信した場合、ホストマシンHMではアクセスコード用の秘密鍵を使用して復号してアクセスコードを得る（ステップS60）。そして、上述のステップS82で照合済みのユーザデータベース10のそのユーザのデータに登録してあるアクセスコード（マシン固有情報を含む）と照合し（ステップS61）、一致すればアクセスコードが正

規のものであると判断する（ステップS62）。そして、受信したマシン固有情報をユーザデータベース10のアクセスコードと照合する（ステップS63）。この結果、一致すれば（ステップS64）、ホストマシンHMは当該クライアントマシンCMを正規登録ユーザのマシンであると確認しアクセスを許可する（ステップS93）。

【0051】なおこのステップS93 においては、更にセキュリティを強化する目的で、アクセスが許可された後に、アクセス毎にアクセスコードを変更してアクセスコードファイルを更新すれば効果的である。また、アクセスコードファイルにアクセス日時を記録してホストのアクセス日時記録と照合して不正アクセスがなかったかを通知したり、前回のアクセス日時をユーザに通知してユーザ側で不正アクセスの可能性をチェック出来るようにすることも可能である。更に、アクセスコードはホストマシンで一つのみを用意しておくことにしてもよいが、上述のようにユーザ毎またはマシン毎に用意する方が好ましい。

【0052】上述のようにしてアクセスが許可されると、クライアントマシンCMには、登録してあるマシン、仮登録のマシン、パスワード認証通過マシン（パスワード認証後、仮登録されなかったマシン）の一覧が表示される。ここで、クライアントマシンCMのユーザは仮登録マシンを正式に登録したり、登録の解除を行ったり、自身のユーザIDを使用した不正アクセスマシンの認定を行ったりすることが可能である。仮登録またはパスワード認証通過マシンをユーザ自身が不正使用者マシンとして認定すると、その情報がホストマシンHMへ送信されてホスト側の不正使用者マシンデータベースに登録される。但し、不正使用者マシンとして認定された回数が一定数を越えた場合に不正使用者データベースに登録するようにしてもよい。そのようにして不正使用者データベースに登録されたマシンは以後はホストマシンHMへのアクセスが不可能になるように対策を講じることが可能になる。

【0053】前述のステップS63 において、ホストマシンHMが受信したマシン固有情報とユーザデータベース10に登録されているユーザIDに対応するマシン固有情報とが不一致であった場合には（ステップS65）、ホストマシンHMはそのクライアントマシンCMに対してはアクセス終了またはクライアントマシンCMの仮登録のいずれかの処理を行なう（ステップS94）。

【0054】このステップS94 は、正規ユーザまたは不正使用者が非登録マシンに最新のアクセスコードファイルをコピーした場合が該当する。この場合には、正しいアクセスコードファイルを使用するようにホストマシンHMからクライアントマシンCMに提示し、アクセス終了か仮登録のいずれかをユーザに選択させる。

【0055】また、ステップS55 においてクライアントマシンCM側にアクセスコードファイルが存在しない場合

には、更にホストマシンHMが受信したマシン固有情報とユーザデータベース10に登録されているマシン固有情報とが照合され（ステップS57）、一致した場合には登録マシンとして認定されてステップS91 で、不一致の場合には非登録マシンとしてステップS92 でいずれも仮登録処理される。

【0056】ステップS91 では、ユーザがアクセスコードファイルを紛失（意図的または過失による削除）していると見なしてクライアントマシンCMの仮登録を行なうが、不正使用者がマシン固有情報を変造した可能性もある。またステップS92 においては、クライアントマシンCMは登録されていないと見なされ、この場合のユーザは正規ユーザである場合と不正ユーザである場合との双方の可能性がある。

【0057】更に前述のステップS61 においてアクセスコードが不正であると判断された場合（ステップS66）、ホストマシンHMが受信したマシン固有情報とアクセスコードに含まれるマシン固有情報とがユーザデータベース10のユーザに対応するマシン固有情報と照合される（ステップS67）。この照合結果は以下のステップS68, S95の処理、ステップS69, S96の処理、ステップS70, S97の処理、ステップS71, S98の処理の4通りに分かれる。

【0058】ステップS68 はステップS67 において、ユーザデータベース10に登録されている情報が受信した情報と一致し且つアクセスコードの情報とも一致した場合である。この場合には、ユーザがアクセスコードファイルを変造した可能性、正規ユーザがアクセスする以前に不正なアクセスがあった可能性、不正使用者がマシン固有情報の変造能力を有し且つ古いアクセスコードファイルを入手した可能性等が考えられる。

【0059】従って、ステップS95 において、アクセスコードファイルが正しくないこと、不正ユーザによるアクセスがあった可能性がホストマシンHMからクライアントマシンCMに提示され、アクセス終了またはマシンの仮登録のいずれかを選択することがユーザには可能である。

【0060】ステップS69 はステップS67 において、ユーザデータベース10に登録されている情報が受信した情報とは一致せず且つアクセスコードの情報とは一致した場合である。この場合には、正規ユーザまたは不正ユーザが非登録マシンを古いアクセスコードファイルをコピーした可能性が考えられる。

【0061】従って、ステップS96 において、正しいアクセスコードファイルを使用するようにホストマシンHMからクライアントマシンCMに提示され、アクセス終了またはマシンの仮登録のいずれかを選択することがユーザには可能である。

【0062】ステップS70 はステップS67 において、ユーザデータベース10に登録されている情報が受信した情報とは一致し且つアクセスコードの情報とは不一致の場合

合である。この場合には、ユーザが別のマシンのアクセスコードファイルを使用した可能性、不正使用者がマシン固有情報を変造する能力を有し且つ別のマシンのアクセスコードファイルを使用した可能性等が考えられる。

【0063】従って、ステップS97において、正しいアクセスコードファイルを使用するようにホストマシンHMからクライアントマシンCMに提示され、アクセス終了またはマシンの仮登録のいずれかを選択することがユーザには可能である。

【0064】ステップS71はステップS67において、ユーザデータベース10に登録されている情報が受信した情報とは不一致であり且つアクセスコードの情報とも不一致の場合である。この場合には、受信情報とアクセスコードとが一致しているのであれば別のユーザIDまたは別のマシンで登録されているユーザからのアクセス要求である可能性が大きい。一方、受信情報とアクセスコードとが異なっていれば、別のマシンで別のアクセスコードファイルを使用して不正ユーザがアクセスしようとしている可能性が大きい。

【0065】従って、ステップS98において、正しいアクセスコードファイルを使用するようにホストマシンHMからクライアントマシンCMに提示され、アクセス終了またはマシンの仮登録のいずれかを選択することがユーザには可能である。なお、上述のように受信情報とアクセスコードとが異なっている場合には、登録情報が一致しないことをホストマシンHMからクライアントマシンCMに提示し、アクセスを却下し、次回の正規ユーザからのアクセスの際に、不正アクセスがあったことを提示してパスワードの変更を促すことが望ましい。

【0066】なお、上述のいずれの場合においても、ユーザがマシンを仮登録するのであれば、ホスト側でマシン固有情報を含む公開鍵を用いてアクセスコードファイルを作成してクライアントマシンCMにダウンロードする。仮登録状態では時間制限付きでアクセス可能にしてもよいし、使用可能な機能、アクセス範囲に制限を設けてもよい。また、初期登録である場合には、仮登録後にオフライン（郵便等）による正式登録確認を行なうようにしてもよい。

【0067】また、不正使用者対応処理では、単純にアクセス拒否するのみでもよいが、ユーザデータベース10を検索してマシン固有情報から不正使用者を割り出したり、不正使用者の電話番号を記録したり、逆探知により所在を追跡したり、不正使用者マシンの固有情報を下ネットワークに通知して各ネットワークでアクセスを防止してもよい。また、電話の発信元の電話番号による認証方法を併用してもよい。

【0068】上述のような本発明のコンピュータネットワークのクライアントマシン認証方法の第3の発明では、通信路の安全性が十分でない場合、またはクライアントマシンCMのマシン固有情報とアクセスコードファイ

ルの双方を第三者が入手し易く、且つ不正使用者がプログラマレベルでソフトウェアに精通している場合には効果が低い可能性がある。

【0069】また、上述のような本発明のコンピュータネットワークのクライアントマシン認証方法の第4の発明では、「通信路の安全性が十分でない場合または通信路の安全性が十分でなく且つクライアントマシンCMの固有情報とアクセスコードファイルの双方を第三者が入手し易い場合」で、且つ不正使用者がプログラマレベルでソフトウェアに精通している場合には効果が低い可能性がある。

【0070】ところで、上述のような本発明のコンピュータネットワークのクライアントマシン認証方法によっても、クライアントマシンCMにおいてマシン固有情報を改竄される場合には対処不可能である。従って、以下においてはクライアントマシンCM内のマシン固有情報の改竄防止策について説明する。

【0071】図8は本発明のクライアントマシンCM、換言すれば本発明のコンピュータシステムのソフトウェアモジュールの構成例を示す模式図である。

【0072】図8において、クライアントマシンCMはハードウェアレベル100、OSレベル110、アプリケーションレベル120の3階層で構成されている。ハードウェアレベル100にはマシン固有情報101が、OSレベル110にはマシンIDサポートAPI(Application Programmer's Interface)111及び相互認証モジュール112が、またアプリケーションレベル120にはマシンID認証モジュール121、相互認証モジュール122、アクセスコードファイル管理モジュール123、アクセスコードファイル124及びユーザID認証シーケンススクリプト125がそれぞれ配置されている。なお、参照符号130はこのクライアントマシンCMの通信ソフトウェアのメインモジュール（以下、通信ソフトメインモジュールと言う）である。

【0073】ハードウェアレベル100のマシン固有情報101はこのクライアントマシンCMのたとえばハードディスク21のHDD-ID31、CPU 20のCPU-ID32等である。OSレベル110のマシンIDサポートAPI 111は、マシン固有情報101を読み出してアプリケーションレベル120のマシンID認証モジュール121へ送信する。このマシンID認証モジュール121は、通信ソフトメインモジュール130からマシン固有情報を送信する必要がある場合に、マシンIDサポートAPI 111にマシン固有情報101を送信させる。

【0074】通常は上述のようにしてマシン固有情報101が読み出されて通信ソフトメインモジュール130によりホストマシンHMへ送信されるが、その場合にはOSレベル110においてマシン固有情報101の改竄が可能である。このため、本発明ではOSレベル110とアプリケーションレベル120との間でのマシン固有情報101の通信に介在して改竄を防止するために、マシンIDサポートAPI 111には相互認証モジュール112が、マシンID認証モジ

ジュール121には相互認証モジュール122がそれぞれ接続されている。

【0075】図9は上述のようなコンピュータシステムのアプリケーションレベル120の相互認証モジュール122とOSレベル110の相互認証モジュール112との間で実行される相互認証手順の手順を示す模式図である。

【0076】まず、アプリケーションレベル120の相互認証モジュール122から認証要求が発せられる(P1)。これに応じて、OSレベル110の相互認証モジュール112がある乱数「R1」を発生してアプリケーションレベル120の相互認証モジュール122へ送信する(P2)。アプリケーションレベル120の相互認証モジュール122では自身でもある乱数「R2」を発生し、この乱数「R2」とOSレベル110の相互認証モジュール112から受信した乱数「R1」との間で所定の演算「 $*$ 」を実行しその結果の値「 $R1 * R2$ 」を生成する。

【0077】以上のようにして生成された演算結果「 $R1 * R2$ 」は乱数「R2」と共にOSレベル110の相互認証モジュール112へ送信される(P3)。これを受信したOSレベル110の相互認証モジュール112では、「 $R1 * R2$ 」と「R1」との間で演算「 $*$ 」の逆演算「 $!*$ 」を実行する。この逆演算の結果得られる値が送信されてきた「R2」であればアプリケーションレベル120からOSレベル110への通信に際してはデータの改竄は行なわれていないことになる。

【0078】逆に、OSレベル110の相互認証モジュール112においても、乱数「R1」と「R2」との間で所定の演算「 $*$ 」を実行しその結果の値「 $R1 * R2$ 」を生成し、乱数「R1」と演算結果「 $R1 * R2$ 」とをアプリケーションレベル120の相互認証モジュール122へ送信する。これを受信したアプリケーションレベル120の相互認証モジュール122、「 $R1 * R2$ 」と「R2」との間で演算「 $*$ 」の逆演算「 $!*$ 」を実行する。この逆演算の結果得られる値が送信されてきた「R1」であればOSレベル110からアプリケーションレベル120への通信に際してはデータの改竄は行なわれていないことになる。

【0079】以上の結果、OSレベル110とアプリケーションレベル120の間での相互認証が完了したことになり、マシン固有情報101を通信ソフトメインモジュール130が読み出して送信しても改竄される可能性はないことになる。

【0080】このようなクライアントマシンCMにおいて通信制御部とマシン固有情報呼び出し部とが相互認証を行なって、不正使用者のプログラムが割り込むことを防止するような相互認証方式をクライアントマシンCMに採用することにより、プログラマレベルでソフトウェアに精通している不正使用者が、ホストへ送信するマシン固有情報を改竄することを防止することが可能になる。

【0081】

【発明の効果】以上のように、本発明のコンピュータネ

ットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン及びコンピュータシステムによればマシン固有情報を使用し、使用するマシンを特定することにより、不正使用者のアクセスを防止し、また不正使用者のマシンを特定することで、以後のそのマシンによるアクセスを全て防止することが可能になる。

【0082】本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン及びコンピュータシステム第1の発明によれば、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報がホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定するので、マシン固有情報を使用して使用するマシンを特定することにより、不正使用者のアクセスを防止し、また不正使用者のマシンを特定することで、以後のそのマシンによるアクセスを全て防止することが可能になる。

【0083】また本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン及びコンピュータシステムの第2の発明によれば、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、予めホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとがホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定するので、マシン固有情報を使用して使用するマシンを特定することにより、不正使用者のアクセスを防止し、また不正使用者のマシンを特定することで、以後のそのマシンによるアクセスを全て防止することが可能になる。

【0084】更に本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン及びコンピュータシステムの第3の発明によれば、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報と予めホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとがホストマシンへ送信され、ホストマシンではデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定するので、マシン固有情報を使用して使用するマシンを特定することにより、不正使用者のアクセスを防止し、また不正使用者のマシンを特定することで、以後のそのマシンによるアクセスを全て防止することが可能になる。

【0085】また更に本発明のコンピュータネットワークのクライアントマシン認証方法、クライアントマシン、ホストマシン及びコンピュータシステムの第4の発明では、クライアントマシンからのアクセス要求時に入力されたユーザIDと共に、自身のマシン固有情報と予め

ホストマシンから送付されている暗号化された自身のマシン固有情報を含むアクセスコードファイルとが公開鍵で暗号化されてホストマシンへ送信され、ホストマシンでは秘密鍵で復号してデータベースを参照してクライアントマシンが正規ユーザのマシンであるか否かを判定するので、マシン固有情報を使用して使用するマシンを特定することにより、不正使用者のアクセスを防止し、また不正使用者のマシンを特定することで、以後のそのマシンによるアクセスを全て防止することが可能になる。

【0086】また上述の各発明によれば、アクセスコードファイルは、クライアントマシンからのアクセス要求に対してホストマシンがアクセスを許可する都度、ホストマシンにより変更されるので、よりセキュリティが高くなる。

【0087】更にまた上述の各発明によれば、クライアントマシン内でのマシン固有情報自体を改竄することが防止される。

【0088】また本発明のコンピュータシステムによれば、ハードウェア階層に保持されているハードディスク、CPU等のIDであるマシン固有情報を外部へ出力する際の改竄が防止される。

【図面の簡単な説明】

【図1】本発明のコンピュータネットワークのクライアントマシン認証方法の実施に使用されるユーザ側のクライアントマシンの構成及びそのネットワーク接続の状態を示す模式図である。

【図2】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第1の発明の手順を示すフローチャートである。

【図3】本発明に係るコンピュータネットワークのク

ライアントマシン認証方法の第2の発明の手順を示すフローチャートである。

【図4】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第2の発明の手順を示すフローチャートである。

【図5】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第3の発明及び第4の発明の手順を示すフローチャートである。

【図6】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第3の発明及び第4の発明の手順を示すフローチャートである。

【図7】本発明に係るコンピュータネットワークのクライアントマシン認証方法の第3の発明及び第4の発明の手順を示すフローチャートである。

【図8】本発明のコンピュータシステムのソフトウェアモジュールの構成例を示す模式図である。

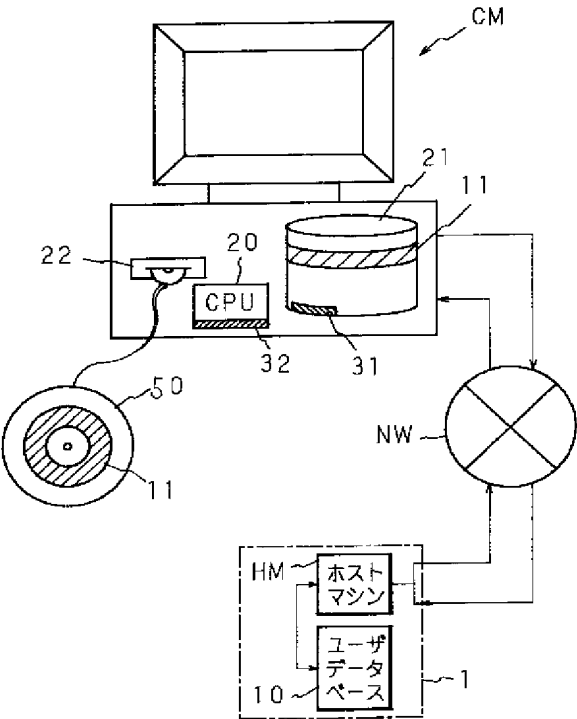
【図9】本発明のコンピュータシステムの相互認証モジュール間で実行される相互認証手続の手順を示す模式図である。

【符号の説明】

CM	クライアントマシン
HM	ホストマシン
NW	ネットワーク
1	通信センタ
10	ユーザデータベース
21	ハードディスク
20	CPU
31	HDD-ID
32	CPU-ID

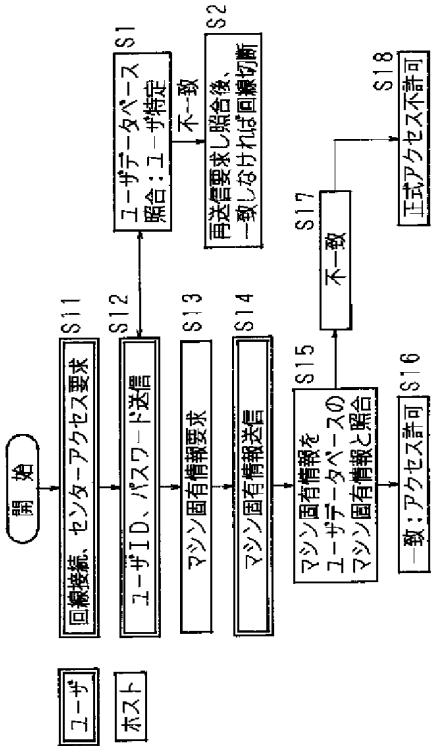
【図1】

本発明のコンピュータネットワークのクライアントマシン認証方法の実施に使用されるユーザ側のクライアントマシンの構成及びそのネットワーク接続の状態を示す模式図



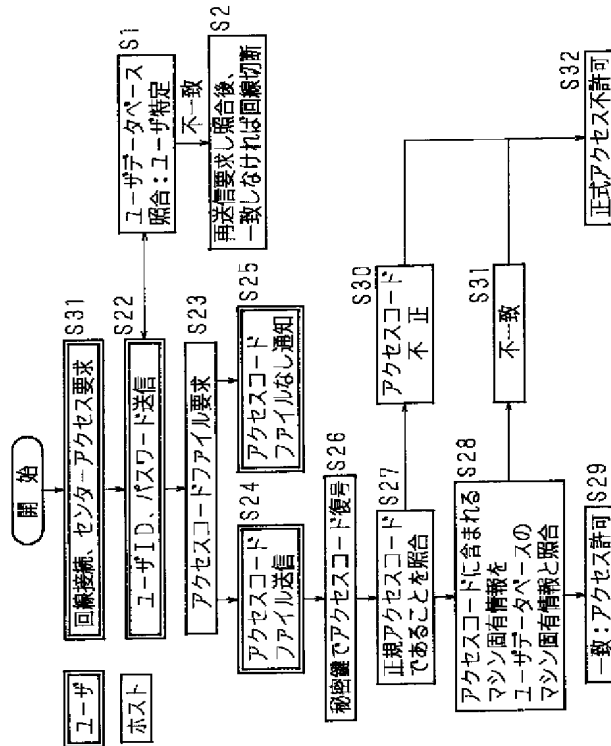
【図2】

本発明に係るコンピュータネットワークのクライアントマシン認証方法の第1の発明の手順を示すフローチャート



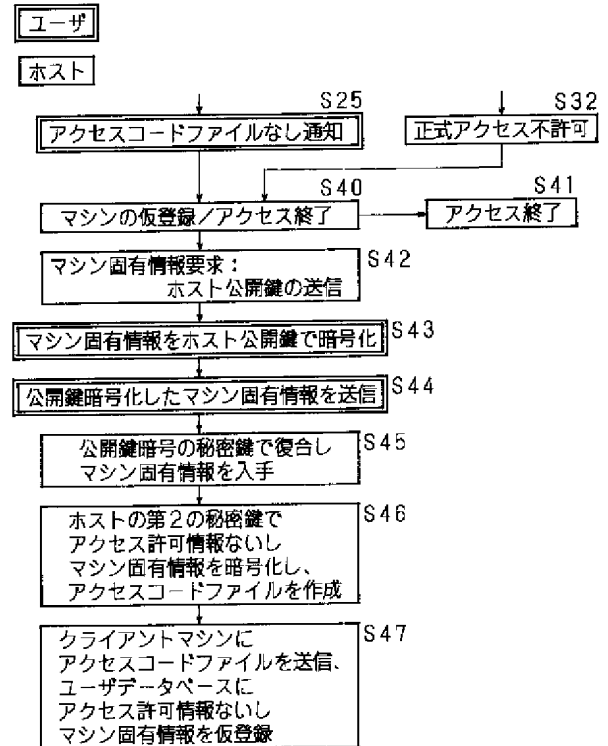
【図3】

本発明に係るコンピュータネットワークのクライアントマシン
認証方法の第2の発明の手順を示すフローチャート



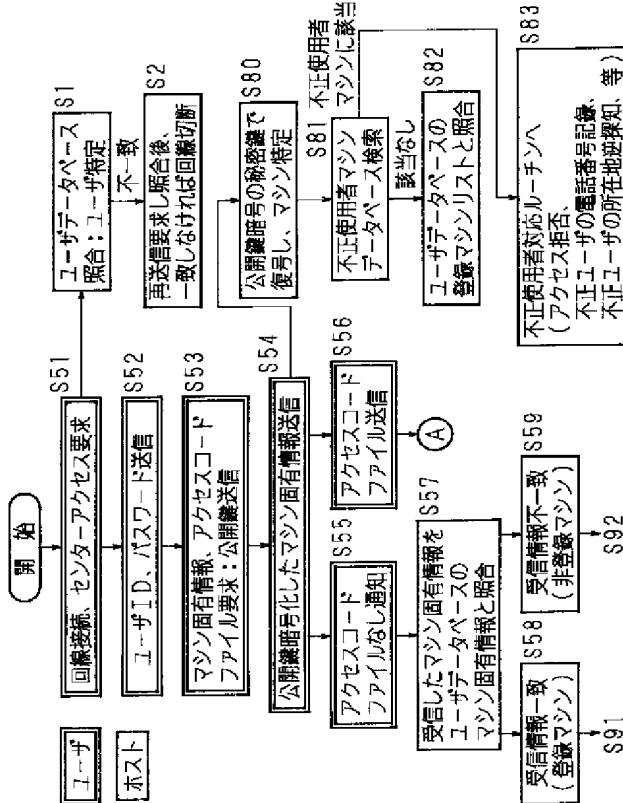
【図4】

本発明に係るコンピュータネットワークのクライアントマシン
認証方法の第2の発明の手順を示すフローチャート



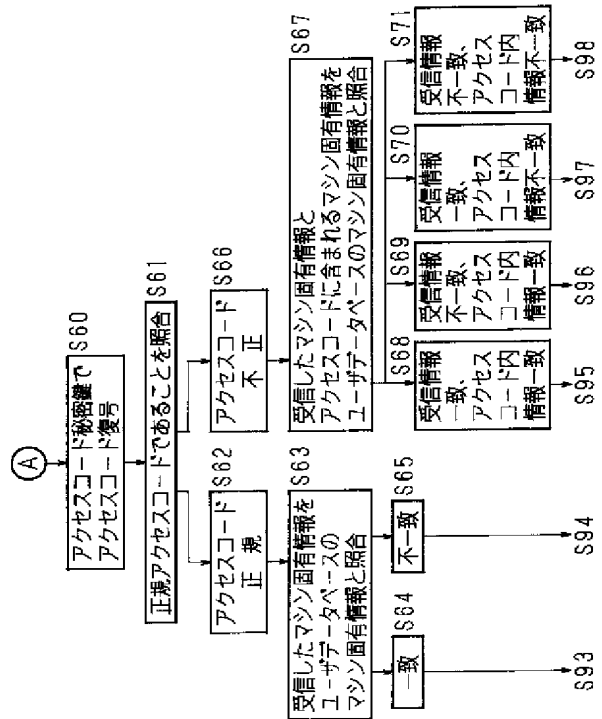
【図5】

本発明に係るコンピュータネットワークのクライアントマシン
認証方法の第3の発明及び第4の発明の手順を示すフローチャート



【例6】

本発明に係るコンピュータネットワークのクライアントマシン
認証方法の第3の発明及び第4の発明の手順を示すフローチャート



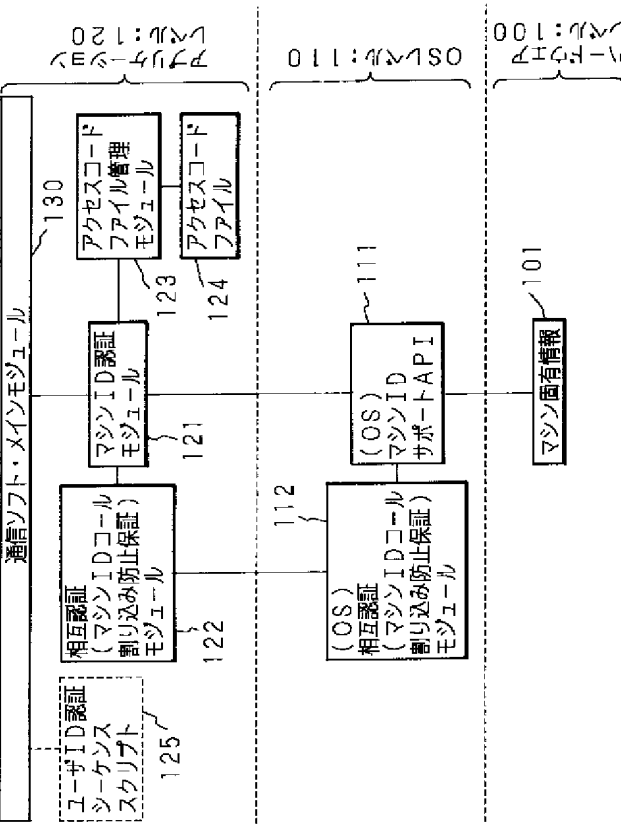
【図7】

本発明に係るコンピュータネットワークのクライアントマシン
認証方法の第3の発明及び第4の発明の手順を示すフローチャート

- S91: アクセスコードファイルの新たな提示し、マシン仮登録ルーチンへ
(ユーザがアクセスコードファイルを削除・紛失した場合、不正使用者がマシン固有情報を変更出来た場合。)
- S92: マシン仮登録ルーチンへ
(非登録マシン。正規ユーザまたは不正ユーザ。)
- S93: 正規登録ユーザと登録。アクセスコードファイル更新。登録/仮登録マシン/パスワード認証通過マシンの一覧表示し、仮登録マシンの正式登録/不正マシン登録/登録解除/パスワード変更を可能。アクセス開始。
- S94: 新しいアクセスコードファイルを使用するよう提示し、終了かマシン仮登録かを選択。
(正規ユーザまたは不正使用者が、非登録マシンに最新のアクセスコードファイルをコピーした場合。)
- S95: アクセスコードファイルが正しくないこと、不正ユーザのアクセスがあった可能性を提示し、終了かマシン仮登録かを選択。
(ユーザによるアクセスコードファイル変造の場合、ユーザのアクセスの前、不正アクセスがあった場合、不正使用者がマシン固有情報を改ざんでき、かつ古いアクセスコードファイルを手でできた場合。)
- S96: 新しいアクセスコードファイルを使用するよう提示し、終了かマシン仮登録かを選択。
(正規ユーザまたは不正使用者が、非登録マシンに古いアクセスコードファイルをコピーした場合。)
- S97: 新しいアクセスコードファイルを使用するよう提示し、終了かマシン仮登録かを選択。
(ユーザが別のマシンのアクセスコードファイルを使用した場合、不正使用者がマシン固有情報を改ざんでき、かつ別のマシンのアクセスコードファイルを使用した場合。)
- S98: 新しいアクセスコードファイルを使用するよう提示し、終了かマシン仮登録かを選択。
(受信情報とアクセスコード内情報が同じ場合、別のID、別のマシンで登録されているユーザによるアクセス要求の可能性大。)
- (受信情報とアクセスコード内情報が異なる場合、別のマシンで、別のアクセスコードファイルを使って、不正ユーザがアクセスしようとしている可能性大。この場合、登録情報が一致しないことを提示し、アクセスを却下し、次の正規ユーザのアクセス時に不正アクセスがあったことを提示し、パスワード変更を要求してもよい。)

【図8】

本発明のコンピュータシステムのソフトウェアモジュールの構成例を示す模式図



【図9】

本発明のコンピュータシステムの相互認証モジュール間で実行される相互認証手続の手順を示す模式図

